IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

LYNN FISH, individually and on behalf of all others similarly situated, Plaintiff, v. WALSWORTH PUBLISHING COMPANY, INC, Defendant.	Case No. 4:24-cv-01651 Jury Demand Class Action

CLASS ACTION COMPLAINT

Plaintiff Lynn Fish ("Plaintiff"), brings this Class Action Complaint against Walsworth Publishing Company, Inc. ("Walsworth" or "Defendant"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") of Plaintiff and other similarly situated customers of Defendant ("Class Members"), including their names, payment card number, expiration dates, and security codes (the "Data Breach").[1]

2. According to the sample notice of data breach filed Defendant with the Vermont and California Attorneys General, Defendant discovery on February 9, 2024, of "a potential data

[1] Exhibit A, Defendant's Notification Letter to Plaintiff.

security incident involving its website and purchasing page."[2]

3. Though Defendant admits that payment information, including security codes and expiration dates, were potentially affected, its notification letter fails to illuminate when the malicious activity took place and how long the hackers had access to Defendant's website and purchasing page. Given that inclusion of this information is standard practice, it is likely that Defendant simply does not know.

4. The lack of information regarding when the hackers first infiltrated Defendant's website and how long they had such access strongly implies that Defendant failed to implement the proper logging, monitoring, and alerting systems necessary to identify malicious activity in a timely manner.

5. After the Data Breach, Defendant sent notification letters to affected individuals in which it offered them access to identity theft protection services, strongly implying that Defendant understands the harm that Plaintiff and Class Members must now face.

6. Moreover, Defendant instructed Plaintiff and the Class to "review your current and past credit and debit card account statements for discrepancies or unusual activity" and to "call the bank that issued the credit or debit card immediately" if they found any such activity.[3]

7. Notwithstanding that Defendant knew about the malicious activity by February 9, 2024, it waited an astounding nine and a half months to notify affected persons. The delay robbed Plaintiff and the proposed Class of an opportunity to protect themselves from fraudulent activity.

---

[2] Office of the Vt. Atty. Gen., https://ago.vermont.gov/sites/ago/files/documents/2024-11-22%20Walsworth%20Publishing%20Company%20Data%20Breach%20Notice%20to%20Consumers.pdf (last visited Dec. 4, 2024); Office of the Cal. Atty. Gen., https://oag.ca.gov/system/files/Walsworth%20Publishing%20Company%20-%20Notice%20of%20Data%20Security%20Event%20-%20CA_0.pdf (last visited Dec. 4, 2024).

[3] *Supra*, note 2.

8. Moreover, the delay was in stark contrast to Defendant's responsibilities under the data breach notification statutes that exist in every state. For example, West Virginia law requires that Defendant's notify affected persons without "unreasonable delay." W. Va. Code § 46A-2A-102(a). The same is true in Missouri. Mo. Rev. Stat. Ann. § 407.1500.2(1)(a).

9. When interpreted what a "reasonable delay" might be, courts should consider that every state that expressly lists a deadline has determined that the deadline should be between thirty and sixty days. Moreover, initial notice to the SEC is four days.

10. Defendant's failure to timely notify affected persons left them blind, unknowing that they faced the significant risk of fraudulent activity such that they could have protected themselves. In other words, many Class Members have lost money and time from fraudulent charges because of Defendant's failure to timely notify.

PARTIES

11. Plaintiff Fish is a resident and citizen of the State of West Virginia, where she intends to remain.

12. Defendant Walsworth Publishing Company, Inc. is a corporation organized under the laws of Missouri, with its principal place of business at 306 N. Kansas Avenue, Marceline, Missouri.

13. Defendant's registered agent is Cogency Global Inc. at 406 N. Main Street, Suite B, Rolla, Missouri, 65401.

JURISDICTION AND VENUE

14. The Court has general subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy is easily more than $5,000,000 and minimal diversity exists. Specifically, the Data Breach affected at least

107,707 people. Minimal diversity exists because Plaintiff is a citizen of West Virginia and Defendant is a citizen of Missouri. Moreover, the amount in controversy is met here because even nominal damages of $50 per Class Member would result in damages of over $5,000,000.

15. This Court has personal jurisdiction over Defendant because its headquarters is in this State.

16. Venue is proper in this Court because Plaintiff resides in this District and Division and a substantial portion of the events giving rise to this Action occurred here.

ADDITIONAL FACTUAL ALLEGATIONS

17. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

18. Defendant made promises and representations to Plaintiff and Class Members that her PII would be kept safe and confidential, and that the privacy of that information would be maintained.

19. Plaintiff's and Class Members' PII was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

21. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep her PII confidential and to protect it from unauthorized access and disclosure.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it

was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

Defendant's Data Breach Was Imminently Foreseeable

23. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

24. Data thieves regularly target institutions like Defendant due to the highly sensitive information in her custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

25. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4]

26. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

27. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

28. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure

[4] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

of the unencrypted data.

29. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

30. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

31. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[6]

32. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[7]

---

[5] 17 C.F.R. § 248.201 (2013).
[6] *Id.*
[7] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

33. For example, PII can be sold at a price ranging from $40 to $200.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

34. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[10]

35. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

Defendant Failed to Comply with FTC Guidelines

36. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for

---

[8] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[9] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

37. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand her network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

38. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet her data security obligations.

40. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security

practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

41. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Failed to Comply with Industry Standards.

42. Experts studying cybersecurity routinely identify institutions that store PII like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

43. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

44. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

45. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

46. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

47. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

48. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to her PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft.

49. Plaintiff and Class Members are at a heightened risk of identity theft, especially because Defendant's failures resulted in Plaintiff's and Class Members' payment card information falling into the hands of identity thieves.

50. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

51. Further, the standard operating procedure for cybercriminals is to use some data, like the payment card information here, to access "fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[12]

52. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to

[12] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

53. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

54. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that her PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

55. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' payment card information is affected.

56. Indeed, as Judge Frank Easterbrook has thoughtfully opined, "plaintiffs have standing because the data theft may have led them to pay money credit-monitoring services, because unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries justify damages, just as they

support standing." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018).

57. And though data breach defendants often attempt to diminish the harm their failures cause, Judge Easterbrook also pointed out that "[l]osing the use of money for three days may be a trifle to some people (though to other it may be a calamity), but a trifling loss suffices under California law." *Id.* at 829.

58. By spending this time, data breach Plaintiff is not manufacturing her own harm. Rather, as Judge Easterbrook explained, she was and is taking necessary steps to set things straight. Moreover, these steps were taken at Defendant's direction.

59. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on her accounts; changing passwords and re-securing her own computer networks; and checking her financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

60. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to her good name and credit record."[13]

61. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect her personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert

[13] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

that lasts for seven years if someone steals her identity), reviewing her credit reports, contacting companies to remove fraudulent charges from her accounts, placing a credit freeze on her credit, and correcting her credit reports.[14]

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

62. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

63. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

64. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard her PII.

Plaintiff's Experience

65. Plaintiff Lynn Fish provided her PII to Defendant as a condition of using its online purchasing site.

66. At the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

67. Plaintiff purchased items on Defendant's website with the understand that her payment card information would be kept secure using commercially reasonable cybersecurity

[14] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

measures and that her payment card information would be free from misuse, including free from disclosure to cybercriminals—as such persons are the exact people from whom the expected cybersecurity controls are designed to protect Plaintiff.

68. Plaintiff's PII was compromised in the Data Breach and stolen by identity thieves and fraudsters who illegally accessed Defendant's network for the specific purpose of targeting the PII.

69. Plaintiff takes reasonable measures to protect her payment card information.

70. Plaintiff suffered actual injury in the form of a severe privacy invasion because of her PII, including her payment card information, falling into the hands of identity thieves whose mission it is to use that information to perpetrate identity theft and financial fraud.

71. Plaintiff suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of her privacy and because she knows she must now face a substantial increase in identity theft and financial fraud attempts.

72. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her name and payment card information, being placed in the hands of criminals whose mission it is to misuse that data.

73. Moreover, Defendant has must continue spending hours of her personal time going through all her past transactions to look for fraudulent activity.

74. Indeed, Plaintiff Fish has had to cancel and get new cards twice due to suspicious activity on her account. This work required her to spend even more time beyond mitigation efforts by working with her bank to address the suspicious activity. Moreover, because she has already

seen the effects of Defendant's failures, she continues to monitor her accounts daily.

75. Further, the stress and anxiety caused by this Data Breach is significantly enhanced because Defendant failed to include any information regarding when the hackers first accessed its website purchasing page, so Plaintiff does not actually know how far back she is supposed to search for fraudulent charges. The lack of understanding and certainty has exacerbated her injuries.

76. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

77. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

78. In addition to the significantly increased risk of identity theft and financial fraud that Plaintiff must now face because of Defendant's failures, and in additional to the significant invasion of her privacy, Plaintiff has already begun to see the effects of the Data Breach.

CLASS ALLEGATIONS

79. Pursuant to the Federal Rules of Civil Procedure 23(b)(1), 23(b)(3), Plaintiff brings this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> All individuals PII was compromised in the Data Breach and to whom Defendant sent an individual notification that they were affected by the Data Breach ("Class").

80. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as her immediate family members.

81. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

82. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

83. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's. The number, however, reportedly exceeds 107,000 individuals.

84. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard her PII;

h. Whether Defendant breached her duties to Class Members to safeguard her PII;

i. Whether hackers obtained Class Members' PII via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members are entitled to damages;

q. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

85. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the

same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

86. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

87. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

88. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating her individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

89. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

90. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send those individuals notification letters.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates the above allegations as if fully set forth herein.

92. Plaintiff and Class Members provided her non-public PII to Defendant as a part of Defendant's offer for online sales.

93. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

94. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

95. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

96. Defendant's duty to use reasonable security measures also arose under the common law, and as informed by the FTC Act, which mandates that Defendant implement reasonable

cybersecurity measures.

97. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that her systems and networks, and the personnel responsible for them, adequately protected the PII.

98. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

99. Defendant had and continues to have duties to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of her PII by third parties.

100. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR, data loss prevention tools, and a centralized security event management system;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove Plaintiff's and Class Members' PII it was no longer required to retain pursuant to regulations; and

f. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

101. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

102. Defendant's violation of the FTC Act also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class Members from the harms associated with data breaches.

103. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

104. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

105. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

106. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

107. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

108. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of her PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

109. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

110. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's decision not to invest enough

resources in its cyber defenses amounts to gross negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

111. Plaintiff incorporates the above allegations as if fully set forth herein.

112. Plaintiff and the proposed Class Members transferred her PII to Defendant as a part of Defendant's offer for online sales.

113. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PII. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members and implicitly agreed to do so.

114. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their PII as a necessary part of receiving healthcare.

115. Defendant, however, failed to secure Plaintiff and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

116. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed it to be provided to Defendant.

117. The contract at least implicitly required Defendant to reasonably protect Plaintiff's and Class Members' PII.

118. Defendant, however, failed to secure Plaintiff and Class Members' PII, as detailed above.

119. Moreover, all contracts include a covenant of good faith and fair dealing in negotiations and in performing the contract, and such good faith requires that Defendant use industry standard, expected, and commercially reasonable means to safeguard the PII that force

their customers to provide—especially knowing the harm that would result from a data breach should it fail to provide such industry standard protections.

120. If Plaintiff and Class Members knew that Defendant had not reasonably secured her PII, they would not have allowed it to be provided to Defendant.

121. Notwithstanding its legal obligations, Defendant failed to implement reasonable cybersecurity measures and thus allowed notorious cybercriminals access to Plaintiff's and Class Members' PII.

122. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

COUNT III
BREACH OF BAILMENT
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates the above allegations as if fully set forth herein.

124. Plaintiff conveyed her PII to Defendant lawfully as a part of Defendant's offer for online sales with the understanding that Defendant would return or delete her payment card information once the transaction was completed and prevent it from being intercepted while it was

in use.

125. Defendant accepted this PII on the implied understanding that Defendant would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiff's PII and act on the PII only within the confines of the purposes for which Defendant collected Plaintiff's PII.

126. By accepting Plaintiff's data and storing it on its systems, Defendant had exclusive control over the privacy of Plaintiff's data in that Plaintiff had no control over whether Defendant's copy of Plaintiff's PII was protected with sufficient safeguards and indeed only Defendant had that control.

127. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendant breached this bailment agreement causing harm to Plaintiff in the form of violations of her right to privacy and to self-determination of who had/has access to her PII, in the form of requiring them to spend her own valuable time responding to Defendant's failures, and in the form of forcing Plaintiff and the Class to face years of substantially increased risk of identity theft and financial fraud.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates the above allegations as if fully set forth herein.

129. Plaintiff and Class Members took reasonable and appropriate steps to keep their PII, including their payment card information, confidential from the public.

130. Plaintiff's and Class Members' efforts to safeguard their own PII were successful, until Defendant failed to protect the same.

131. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and

were entitled to the protection of this information against disclosure to unauthorized third parties.

132. Defendant owed a duty to its customers, including Plaintiff and the proposed Class Members, to keep their PII confidential.

133. The unauthorized release of PII, including payment card information with its attendant security information, is highly offensive to any reasonable person.

134. Plaintiff's and Class Members' PII is not of legitimate concern to the public.

135. Defendant knew or should have known that Plaintiff's and Class Members' PII was private, as any reasonable person would.

136. Defendant caused the publicized of Plaintiff's and Class Members' PII to cybercriminals by failing to implement reasonable cybersecurity measures while being substantially certain that such a failure would lead to a data breach.

137. Indeed, such substantial certainty is clear given the ubiquity of data breaches.

138. Moreover, the disclosure meets the definition of a publication because the disclosure was done to the exact people from whom cybersecurity measures are meant to protect Plaintiff and the Class—such that those identity thieves and fraudsters are in a special relationship with Plaintiff and the Class.

139. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiff and Class Members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiff's and Class Members' privacy by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train her security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate

based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess her respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the

class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a trial by jury on all issues so triable.

Dated: December 6, 2024

Respectfully submitted,

/s/ Colleen Garvey

Colleen Garvey (MO #72809)
Grayson Wells (MO # 73068)
STRANCH, JENNINGS & GARVEY, PLLC
Peabody Plaza
701 Market Street, Suite 1510
St. Louis, MO 63101
Tel: (314) 390-6750
gwells@stranchlaw.com
cgarvey@stranchlaw.com

J. Gerard Stranch, IV*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com

* *Pro Hac Vice applications forthcoming*

Counsel for Plaintiff and the Proposed Class